PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G06F 17/30 | A2

(11) International Publication Number: **WO 00/68841**

(43) International Publication Date: 16 November 2000 (16.11.00)

(21) International Application Number: PCT/US00/12887

(22) International Filing Date: 12 May 2000 (12.05.00)

(30) Priority Data:
60/133,757 12 May 1999 (12.05.99) US

(71) Applicant *(for all designated States except US)*: iWITNESS, INC. [US/US]; Suite 2N, 2995 Wilderness Place, Boulder, CO 80301 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: LAMBERT, Francis, T. [US/US]; 1901 Spruce Street, Boulder, CO 80302 (US).

(74) Agents: SABETT, Randy, V. et al.; Cooley Godward LLP, One Freedom Square–Reston Town Center, 11951 Freedom Drive, Reston, VA 20190–5601 (US).

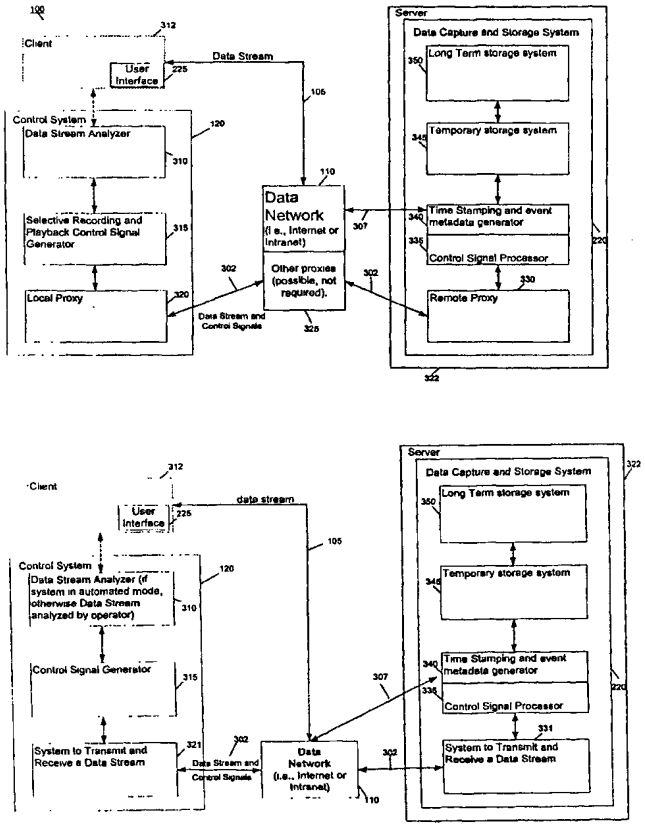
(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: INTERACTIVE DATA STREAM RECORDING SYSTEM

(57) Abstract

A data recording system is disclosed that allows for selective recording of elements of a data stream. The data recording system can include a data stream processing system. The data stream processing system can further include a data capture and storage system, and a control system. The recording system can be controlled either by a user interface or by a separate automated system. The recording system can also operate in a single computing device, or it can operate over a data network. The control system generates control signals that cause the selected data from the data stream along with associated metadata to be recorded in a storage system. The metadata can include information about the external context of the overall data processing system that includes the data recording system. The metadata can also include such things as the time and date, the serial number of the media, or a file number. Also disclosed is a method for selectively recording data from a data stream, and storing the selected data and associated metadata in a verified data object (VDO). The VDO can be used for verifying various types of compliance.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERACTIVE DATA STREAM RECORDING SYSTEM

Inventor: Francis T. Lambert

RELATED APPLICATION

The present application claims priority to Provisional Application No. 60/133,757, filed May 12, 1999, which is incorporated herein by reference in its entirety.

BACKGROUND

Field of the Invention

This invention relates to a data recording system and to methods for producing and using the same. More specifically, the invention relates to a data recording system having a data capture system controlled by an event response system that allows a user or another system to select which data is being captured and subsequently submitted to storage for recordation.

Description of the Related Art

The advent of electronic data interchange, the growth of electronic communications, and the growth of the availability of information and e-commerce on the World Wide Web has prompted an increasing number of computer users and computer systems to employ processes that store records of transmitted or received data. The stored data can include, for example, database files, electronic documents, e-commerce transactions such as stock trades or merchandise purchases, and the like, all of which provide records of activity performed over data networks. Typical data

network communications systems generally include data capture systems, which allow storage of data transmitted over networks. The typical data storage systems usually captures and stores data that are transmitted or received by it in conjunction with another data source. These systems generally record the entire data stream or files specified to be recorded or "downloaded" onto a storage device on the receiving system. For example, the WebVCR application, designed and distributed by NetResults Corporation, allows a user to download and store web pages stored as a web site on a web server. Similarly, the BlackWidow application, designed and distributed by SoftByte Laboratories, performs a similar function. However, these systems are somewhat limited in that they only allow the capture of a static storage of web pages available for download from a server. They cannot record a data stream consisting of interactions between users, servers, processes, and pre-composed web pages and forms, such as occurs during an e-commerce transaction or during interactions with other types of data processing devices. These systems also do not allow the recording as a single event in time a data stream comprised of data sent and received from multiple web servers.

Additionally, a modern data network transmission, such as one that could occur during an electronic commerce ("e-commerce") World Wide Web ("Web") session, may contain a large volume of data containing inconsequential information that, if stored, would inefficiently use data storage resources on a user's terminal. It is also possible that the volume of useful data in the network data stream is too large for the user terminal to efficiently store, and that it would be desirable to have another system with additional storage capacity able to both read the data stream and selectively record elements of its based on control signals from a controlling user or system.

As a result, the party receiving the data may not wish to record all of the received data, and may find it more desirable to selectively record only those parts of the data that they deem important enough to record. Alternatively, the receiving party may wish to enable a separate storage capture and recording system to selectively record network data under the receiving party's control. Efficient use of data storage capacity is, in large measure, dependent on that ability of the storing party to control the location, type and amount of data that is being stored. Thus, to efficiently use storage for the recordation of transmitted data, it is often desirable to selectively control which data are recorded at the time data are transmitted. Unfortunately, current data network recording systems fail to provide a means for those users or systems transmitting and receiving data to interactively and selectively record elements of a data stream based on a user action, or based on certain contents of the data stream, such use of encryption or contents of Web pages. In most cases, due to a lack of interactive data recordation control, the recording entity must store data which it finds less useful, thereby wasting storage resources and complicating stored data management.

In addition, current systems do not allow for efficient and accurate auditing and verification of electronic transmissions. As the number of electronic transmissions, and particularly electronic transactions, continues to increase, a means for electronic vouching of the transmissions and interactions of users, servers, and processes becomes a necessity for proving the accuracy and existence of an electronic event.

Furthermore, with downloaded data objects, the systems exchanging data must pre-define those objects and the protocols by which they will be transmitted. Data occurring in a network data stream which generates a spontaneous, or not previously defined, response or meaning for one of the parties to the transmission is generally not

available to be captured and stored as a "downloadable", "replayable", or "analyzable" data object that contains information about the content of the transmission as well as information about the transmission, known as "metadata". Metadata allows systems to use selectively recorded data streams to establish evidence of an electronic event to be used for purposes of auditing, dispute resolution, information management, and other forms of data analysis. Moreover, with network data streams that are encrypted by keys known only to the sending and receiving parties or systems, any external data recording system is required either to store the keys or to store the selected data in an un-encrypted form, so as to allow later reading of the recorded data by authorized accessors. Consequently, a need exists for a data recording system that overcomes the foregoing drawbacks.

SUMMARY OF THE INVENTION

The present invention provides a data recording system that allows for selective recording of elements of a data stream. The control of recording of the data can be provided through a control system that is integrated into the data stream processing system of the controlling entity. The control system may be part of an interactive user interface manipulated by actions performed by a human computer operator, or it may be part of a data processing system, such as a web server or other data gathering, sending or receiving devices, that interprets the content of the data stream to trigger one or more control signals to the data recording system. The entire recording system may be contained within the user system or in data processing systems, or parts of it may be in an external system controlled by signals transmitted to it over a network.

The control system may interact with a user interface implemented either as a standalone computer application, or integrated into other applications such as a web browser or word processor, or it may be an automated process that executes on a data processing system such as a web server.

The data recording system provides a convenient and easily used system for controlling the capture and storage of only those parts of a data stream which the using entity finds desirable to record. Such a data recording system can include a mechanism that permits subsequent verification of a transmission or transaction. This can be useful in any situation requiring authentication or auditing of a transaction or transmission.

The data recording system allows for the recording of metadata, or information about the data stream content and the context of its occurrence. It allows this data to be stored with the recorded data stream content in a self-contained "data object".

The system also allows data to be selectively recorded based on particular criteria, including but not limited to patterns within the data stream, transmission information such as data stream addressing, external events such as time and date, data stream formats such as SSL encryption, or other attributes of the data that could cause a human user or automated process to desire to record a portion of a data stream.

Additional aspects and embodiments of the present invention will become apparent upon a review of the following detailed description and accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 depicts a basic system for selective recording of data, according to the present invention.

Fig. 2a depicts a system for selective recording of data that includes an external system for controlling the selective recording of data.

Fig. 2b depicts a system for selective recording of data that contains an automated means for controlling the selective recording of data.

Fig. 3a is a detailed block diagram of one embodiment of a system for selectively recording data involving an intermediary.

Fig. 3b is a detailed block diagram of another embodiment of a system for selectively recording data.

Fig. 4 is a block diagram of an embodiment of the present invention embedded in a server.

Fig. 5 is an example of a Functional Relationship Diagram used in an embodiment of the present invention.

Fig. 6 is an example of a Data Object Table used in an embodiment of the present invention.

Fig. 7 is an example of a Control Message Table used in an embodiment of the present invention.

Fig. 8 is an example of a user interface showing an embodiment of the present invention.

DETAILED DESCRIPTION

As communications technology continues to evolve, the amount of information travelling over data networks increases very quickly. Many factors contribute to this growth, including the amount of extraneous or overhead information needed for the various communications protocols in use. A data recording system according to the

present invention can selectively record only those data elements that a user desires and can exclude from the recording process any unnecessary or undesired information.

As shown in Fig. 1, a data recording system 100 according to the present invention can allow selected data elements from data stream 105 that originate from data network 110 to be recorded in long term data storage 125. Data stream 105 can consist of raw data that travels over any type of data communication medium, wherein raw data means data that may contain the data items needed or desired by the user along with certain extraneous or unneeded pieces of data. Data recording system 100 can include a data stream processing system 115 for determining those data elements from data stream 105 that are to be recorded in long term data storage 125. Data stream processing system 115 can further include a control system 120 for providing control over the recording of the data elements in long term data storage 125.

Fig. 2a provides a more detailed block diagram of data recording system 100, which can include a data capture and storage system 220. Data capture and storage system 220 can contain data capture system 205 and data storage system 210 within the overall data stream processing system 115. Data elements from data stream 105 can be captured by data capture system 205 and held for processing in a data buffer. Based on that processing, control system 120 can selectively control those data elements that are passed to data storage system 210 for ultimate storage in long term data storage 125. Data storage system 210 can transfer captured data into a storage device such as long term data storage 125. Referring back to data capture system 205, it can comprise, for example, a computer connected to data network 110 over which data stream 105 is transmitted, which contains a hard drive upon which the selected data is recorded, while data storage system 210 can comprise, for example, a tape storage device

connected to data network 110. The system in Fig. 2a can also include a control system 120 to allow a controlling entity to start, stop, or pause the data capture process by data capture system 205 and to allow a controlling entity to write, read, view, edit, or delete the captured and stored data from long term data storage 125. Additionally, the capability to alter the recorded data after being captured may be limited, which could allow it to function in evidentiary or audit trail capacities. Similarly, viewing of the recorded data and the stored data can be limited by access control systems. Also, the system can further log access, use, and data management events associated with the data object and integrate those events with the data object record.

Fig. 2a also shows a data recording system that can utilize user interface 225 for interacting with control system 120 to control the data that data storage system 210 passes to long term data storage 125. User interface 225 can allow a human operator to assess the information (in the form of data elements) received from data stream 105. Based on the decisions and subsequent manipulations by the human operator of user interface 225, signals can be generated that capture and store those elements of the data stream that the operator chooses to capture and store. Control system 120 can then selectively pass information to data storage system 210 for ultimate storage in long term data storage 125. For example, during an electronic transaction, a user (either individual or corporate) might want to record the entire "transaction experience", including all photos or graphics that were displayed by a merchant during the session, all text, all input by the user, and the date and time information. However, the user might not be interested in such data as, for example, the extraneous advertisements that the merchant would also display to the user during the course of the transaction. Thus, the user could utilize the present invention to only preserve the information that the

user considers relevant to the transaction. Alternatively, a merchant could use such a system in a very similar manner to retain a verifiable record that the user actually conducted the transaction.

Alternatively, as shown in Fig. 2b, user interface 225 can be eliminated from the system and an automated data processing system within control system 120 can process the data stream without direct human intervention. The automated data processing system can include a system that generates recording control signals in response to an automated analysis of the data stream content. Such analysis can result in controls that are generated for a number of reasons, including in response to such things as pre-defined values or patterns; external events, such as the time or date; data stream addressing or URL designators; or data stream format, such as Secure Socket Layers (SSL) encrypted transmission. The signals generated by this automated data processing system can control the other systems that selectively capture and store elements of the data stream.

In addition to systems where the recording and storage systems are co-located, another embodiment of the present invention shown in Fig. 3a contains a data capture and storage system 220 within server 322 that can be connected to data network 110, to which control system 120 is remotely connected. In this embodiment, data capture and storage system 220 can be an intermediary in the transmission of the data, similar in function to a proxy server, which acts as an intermediary data transfer agent by receiving data, optionally conditioning it, and then transmitting the data onto the same or another network. Remote proxy 330 within data capture and storage system 220 can receive recording control signals or messages contained within data stream and control signals path 302, which can be transmitted over data network 110 from remotely

located control system 120 to data capture and storage system 220. Control signal processor 335 can interpret the recording control signals or messages to cause timestamping and event metadata generator 340 to generate metadata acquired, for example, over data path 307 from data network 110. This metadata and the selected data from data stream and control signals path 302 can then be stored in temporary storage 345, which can then ultimately be stored in long term storage system 350.

Remotely located control system 120 can include one or more automated data processing applications running on an automated data processing system, including data stream analyzer 310. Remotely located control system 120 could also include any other system designed to generate recording control signals to a separate data capture and storage system on a network. Alternatively, remotely located control system 120 can be connected to client 312 containing software user interface 225 through which a human operator can cause control signals to be generated.

A data recording system 100 as shown in Fig. 3a can comprise a number of different components, including but not limited to client 312, server 322, and one or more proxies 325. Client 312 can include any communications technique used to provide information to the user from the system. In one embodiment, client 312 can be a browser (i.e. a commercial software package used for browsing the contents of the Web). Similarly, server 322 can include a software package with which the browser can communicate. Server 322 can provide content to a user, in response to user transmissions of requests over Uniform Resource Locators (URLs or links). In one embodiment, proxy 325 can consist of a device that receives data from the network, optionally conditions or processes it in some way, and the transmits the optionally conditioned data onto the same or another network.

The user can retrieve one or more segments of content from server 322. Each segment can consist of such things as, for example, images, text, and other links, along with any other types of data item that can be delivered via the transmission medium. In one embodiment, the transmission medium can be over the Web wherein a segment would be a Web page.

Through the use of several communications messages (further described below), a user can store recordings of one or more segments of the data stream. These recordings can be stored in any appropriate medium, including any combination of short term storage or long term storage. Once stored, the recordings can later be stored in an archive for additional storage security.

In one embodiment involving proxies, proxy 325 can act as an intermediary between communicating data terminals for the data stream to be selectively recorded. Data capture and storage system 220 within server 322 can be connected to proxy 325, which allows selective recordation of the data stream passing through the intermediary system. Control system 120 can transmit recording control signals or messages through proxy 325. Additional intermediary data receiving and transmitting systems, or proxy servers, can be placed at various points in the network that is carrying the data stream. This "multiple proxy" system can enable, for example, encrypted data communications between the proxy and control system 120 in those cases where control system 120 would be unable to control the encryption of data transmitted directly to the data capture and storage system 220. A common instance of this often occurs with Web browser transmissions through sophisticated firewall applications. The control system can send unencrypted control signals and data stream information to the second

intermediary system, which can then selectively encrypt the control signals and data stream information for transmittal over a public network to the data recording system.

In yet another embodiment shown in Fig. 3b, the data stream to be selectively recorded is echoed to data capture and storage system 220 for purposes of capture and storage according to signals generated by control system 120. Control system 120 analyzes data stream 105 to determine the proper control signals (or messages, as discussed with regard to Fig. 7) to put in data stream and control signals 302. Following transmission by data stream transmission reception system 321 and receipt by data stream transmission reception system 331, control signal processor 335 in data capture and storage system 220 can analyze the data stream to extract the control signals to determine how to manipulate and process the data. Control signal processor 335 can interpret the recording control signals or messages to cause timestamping and event metadata generator 340 to generate metadata acquired, for example, over data path 307 from data network 110. This metadata and the selected data from data stream and control signals path 302 can then be stored in temporary storage 345, which can then ultimately be stored in long term storage system 350. This embodiment provides added value in network environments since it does not place further the further burden on the system in the form of an added proxy.

Fig. 4 depicts a functional block diagram of an embodiment of the present invention which shows one aspect of the CommCorder, designed by iWitness, Inc., of Boulder, CO. The CommCorder can include client 405, which can consist, for example, of a browser, such as the well known Internet Explorer, designed and manufactured by MicroSoft, Inc. Under the control of a human user, client 405 can communicate with application server 430 through secure web server 415 and

CommCorder proxy 425. Client 405 can use the well known Hypertext Transmission Protocol (HTTP) over a Secure Sockets Layer (SSL) connection to establish a secure data link 410 with secure web server 415. CommCorder proxy 425 can provide standard web server interface 422 over which secure web server 415 can communicate. Similarly, CommCorder proxy 425 can provide standard web server interface 426 via which application server 430 can communicate. Thus, CommCorder proxy 425 emulates a web server interface both to application server 430 and to secure web server 415.

In doing so, client 405 can communicate with application server 430 by securely sending data using SSL over a data network (such as the Internet) to secure web server 415. That data can then be decrypted by secure web server 415, sent over standard web server interface 422 to CommCorder proxy 425 where it can undergo further processing. Finally, the data can then be sent over standard web server interface 426 to application server 430. Once received, the data can be processed by application server 430. Both standard web interface 422 and standard web server interface 426 can be implemented using any well known interface method, including the Netscape Server API (NSAPI) (designed and produced by Netscape, Inc.), the Internet Server API (ISAPI) (designed and produced by Microsoft, Inc. of Redmond, WA), or StrongHold, a third party product that provides secure web server functionality using SSL.

As an example, during an e-commerce transaction a user might request information on a certain product from application server 430. Although to the user that request would appear to be sent directly to application server 430, in an embodiment of the invention, it would actually travel through secure web server 415 and CommCorder proxy 425. In response to the request, application server 430 would send the data about

the requested product (i.e., the response data) through CommCorder proxy 425 and secure web server 415 over HTTP connection 410.

Since all data passes through CommCorder proxy 425, it can cause the data and metadata (which are additional data items that describe the nature of the recorded content) to be placed in a queue for eventual processing by Verified Data Object (VDO) engine 445. VDO engine 445 can run continuously at the server, reading data and metadata from the input queue, discarding unneeded messages, reconstructing transactions (if needed), creating one or more VDOs, and sending the VDOs to archive manager 455. Archive manager 455 can be any optional external system that manages the storage and retrieval of VDOs for later playback or retrieval.

A VDO can contain be created from several different types of metadata. For example, data from a network can be combined with metadata that provides information about one or more aspects of the external context of the overall system that utilizes a data recorder according to the present invention. Alternatively, data from a network can be combined with metadata that provides information about one or more aspects of the internal system. Internal system data could include such information as a serial number or machine identification number of the computer containing the recording system, or a serial number of the media on which the VDOs can be stored. In yet another embodiment, metadata could be used that provides information that would be useful for records management purposes, such as a file number or identifier, or for access control purposes, such as a user name and privilege information. One additional type of access control metadata could include data for the use in digitally auditing electronic records.

VDO engine 445 can scan the queue at regular intervals for data and metadata to process, or can begin processing immediately if a queue threshold is crossed. VDO engine 445 can utilize a number of different protocols to communicate with archive manager 455 over data path 450, such as the well known HTTP. It can also use any appropriate proprietary protocol, such as any VDO-specific communications protocol.

Also, in an alternative embodiment, the user can establish a non-secure connection directly with CommCorder proxy 425. In this example, the connection between client 405 may or may not be secured. If it is secured, CommCorder proxy 425 could participate in the knowledge of any cryptographic keys needed to secure the transaction. In yet another alternative embodiment, prior to being sent to archive manager 455, VDO engine 445 could further process the VDOs to make them compatible with legacy computer systems, including but not limited to those that use electronic data interchange (EDI). VDO can accomplish this by converting the VDO to the necessary alternative data formats required for compatibility with the legacy system.

Fig. 5 depicts a functional relationship diagram of an embodiment of the present invention showing the various states in which the system can function and the transitions from one state to the next during a particular user session. In Ready/Pre-recording state 505 the system can receive information over data stream and control signals path 302. In this state, data from data stream and control signals path 302 can be stored in a temporary buffer.

Upon receiving a Start Recording signal from data stream and control signals path 302, the system can transition to Record state 515. In this state, depending on the performance of the system and its ability to process the incoming data stream, data

from either the temporary buffer or directly from data stream and control signals path 302 can be written over data path 525 to short term storage 520. In addition, a time stamp and other metadata can be generated. As the system remains in this state, data and associated metadata can continue to be written to short term storage 520.

Upon receiving a Stop Recording signal, the system can transition to Review state 535. In this state, the system can transmit recorded data to a display in a user interface for review by a human operator in Playback state 545. In Playback state 545, the human operator can control the playback process and can choose selected portions of the data stream to review. From Playback state 545, the human operator can then review and process the data stream in Process state 555. Also in Playback state 545, the human operator can specify record identifier 560, which can cause the system to enter Retrieve mode 565 where recorded data from long term storage 125 can be moved into short term storage 520 in preparation for later review.

Also in Review state 535, Delete signal 570 can be issued, causing the recorded data stream and metadata to be removed from the data buffer, short term storage 520, or long term storage 125. Further, Commit signal 585 can be issued in Review state 535, causing data from the data buffer or short term storage 520 to be transferred to long term storage 125. In addition to allowing playback for a human user, other embodiments can allow automated processes to utilize a retrieval mode to read and analyze stored data.

Fig. 6 depicts the Verified Data Object (VDO) structure 600 of the present invention. VDO structure 600 depicts the relationships that can exist between the various data objects contained in data recording system 100, including the recorded

data stream content 602 portion of the VDO and the Metadata objects portion 604 associated with selected data stream content 602.

In order to delineate diverse segments of the recorded data stream, the VDO content portion 602 can consist of Sequence Markers 615 containing properties 620, which can include SegmentReference, StartTime, and EndTime, and which describe in a one-to-one relationship Segments 625 of recorded data stream data. VDO Content 602 can contain an indeterminate amount of Segment Objects 625, which is dependent on the amount of data selectively recorded from the data stream. Segment objects 625 can contain properties 630 that further describe the recorded data segment 625, such as ID, Request and Response Data used by Web servers, and the recorded data stream data itself. Use of Sequence Markers 615 and Segment objects 625 allow indexing and searching algorithms to quickly locate a portion of the recorded data stream within the content portion 602. Sequence Markers 615 also allow a VDO 600 to mark data recorded data stream content in a way that is useful to data analysis or playback. An example of this would be the demarcation of web pages within a stream of HTTP or HTML data for later display of the web pages as they occurred in the original recorded data stream event.

Figure 6 additionally shows the Metadata objects 604 associated with content 602. Metadata objects provide information that allow users and processes to better understand, manage, and process the content 602 of VDO 600.

VDO 600 can contain many types of metadata objects 604, examples of which are shown in Figure 6. One example is Session object 605 that contains Properties 610. Properties 610 provide information about recorded content 602 that allows users and processes to organize the VDO 600 itself, including SessionId, which can contain a

unique identifier for the present data recording session, Session Name, a textual description of the recorded data, User Name, the name of the creator of the VDO, and Start and End Time, which allow the users to organize VDOs chronologically.

Another example of VDO Metadata objects 604 is the Access Object 645, which contains properties 650 that provide information for logical control of the access to and management of VDO content and metadata. There can be multiple Access Objects associated with a VDO that allow multiple users and systems to access and process the VDO. Access object properties 650 can contain values such as User Name, which allow identification of an authorized user of the VDO, Authentication Token, which provide the data that the user must provide to access the VDO, such as a password or Digital Certificate, and a list of rights that the accessor has with the associated VDO, such as Can Read, which allows the user to view the VDO, or Can Retrieve, which allows the user to download the VDO to another system. Other Access object properties 650 can be added to provide additional security, privacy, and confidentiality for the content and metadata in the VDO.

Another example of VDO Metadata objects 604 is the Integrity Object 648, which contains properties 653 that provide information for checking the validity of stored VDO content and metadata. Integrity object properties 653 can contain values such as Hash Value, which contain a calculated numerical digest of the original VDO data. The stored Hash Value can be used as a comparison to recalculated Hash values that can ascertain the validity of stored VDO data. Integrity object properties 653 can also contain values such as Date Checked, which provide a log of validity checking events and the results thereof. Other Integrity object properties 653 can be added to

provide additional assurances as to the validity of the content and metadata in the VDO. This could include, for example, a digital signature value.

Another example of VDO Metadata objects 604 is the Audit Object 645, which contains properties 650 that provide information supporting auditing of stored VDO content and metadata. Audit object properties 650 can contain values such as Vouch Type, which describe the type of audit document contained in the VDO data, or VDO Link, which can provide a pointer to related VDOs, thereby creating an automated electronic audit trail among diverse stored VDOs. Other Audit object properties 650 can be added to provide additional means by which to assist in the process of using the content and metadata of a VDO in an audit, such as a financial or system audit.

Another example of VDO Metadata objects 604 is the Retention Object 635, which contains properties 640 that provide information supporting disposition and destruction of stored VDO content and metadata. Retention object properties 640 can contain values such as Destroy Date, which describe the date and time at which the VDO data will be deleted automatically, or Authorized Manager, which can provide identification of users and systems that are authorized to change or override a Destroy Date event. Other Retention object properties 640 can be added to provide additional means by which the content and metadata of a can be managed as a time sensitive electronic record.

Another example of VDO Metadata objects 604 is the Externals Object 636, which contains properties 641 that provide information gathered from external sources that provide additional meaning to the VDO content and metadata. Externals object properties 641 can contain values such as Detail Data, which contain the data value that has been acquired from sources external to the recorded data stream. Detail Data values

could include stock prices, weather, political events, or other information that gives additional meaning to the VDO content and metadata. Other Externals object properties can include Detail Description, which provides an explanation of the Detail Data value, or Detail Time, which describe the date and time at which the external data was acquired. There can be multiple Externals Objects 636 associated with a VDO that provide additional meaning to a VDO. Other Externals object properties 641 can be added to provide additional types of information relating to the VDO contents and metadata.

Figure 7 shows examples of the types of control messages can be used between the entities to facilitate system operation and the properties that they can communicate to the control signal processor in the data capture and storage system. These can include messages for session recording creation control, session playback control, session storage control, and general session management. For example, general session management messages can be used throughout the operation of a session during any of the states of the system described above to control the attributes of a selective data stream recording session.

Examples of session recording creation control messages shown in Figure 7 include Start Recording 712, Stop Recording 728, Pause 784, Start Segment 790, Commit 752, and Delete 768. The recording creation control message can also control the use of a data capture system buffer, which allows the system to retain stream data that occurred before the transmission of a Start Recording message 712, and allows for otherwise unrecoverable data to be included in a Session VDO content segment 602.

Examples of session playback control messages shown in Figure 7 include Playback 736, Next Segment 744, Previous Segment 760, First Segment 767, Last

Segment 742, and Pause 784. Additional messages beyond those shown on Figure 7 can include messages instructing how the session is to be played back.

Examples of session storage control messages shown in Figure 7 include Get Record Name 720, Commit 752, Delete 768, Rename Session 794, and Get Session List 796. Additional storage control messages can include Edit Access, Edit Retention, Add Externals, Show Audit Trail, and Check Integrity, or other messages that allow the system utilize the content 602 and metadata objects 604 to manage the storage of VDO 600.

Additional messages can be used for general session management beyond those shown in Figure 7. Examples of general session management messages that can be used to manage other aspects of selective data stream recording include user login, end session, get session state, reset session state, and set session cache size.

RECORDING CONTROL MESSAGES

Examples of recording creation control messages can be used by the control system 120 to inform the data capture system 205 as to which portions of the data stream system 105 that the control system 120 chooses to pass to the data storage system 210.

The Start Recording message 712 can be used to tell the system to start capturing segments 630 of data stream 105. The system can use a "cached segments" property to determine the number of previously captured segments prior to the sending of a Start Recording message 712 to include in this session 605. A Start Recording message can have the properties 716 of Session ID, which uniquely identifies this capture and recording Session, Cached Segments, which gives the number of segments cached prior to the Start Recording message to include in the Session, and Session Name, which provides a human or machine readable label for the captured data.

The Pause message 784 can be used to tell the system to pause the capture of data stream segments during the capture phase of Session creation. A Pause Record

message can contain the properties 788 of Session ID, which uniquely identifies this Session, Pause Start Time, which gives the time at which the Pause in capture started, and Pause Stop Time, which gives the time at which the Pause in selective data stream capture ended.

The Stop Recording message 728 can be used to tell the system to stop the capture of data stream segments during the capture phase of Session creation. A Stop Recording message can contain the properties Session ID, which uniquely identifies this Session, System Time, which gives the time at which the capture ended, and Segment Marker, which gives a pointer to the last segment at the time the selective data stream capture ended.

The captured data can then be moved into a pre-commit state in which it can be reviewed or labeled by a user or process.

The Start Segment message 790 can be used by the control system 150 to delineate to the capture system 205 where within the data stream 105 a segment selected for recording begins. For example, this data stream segmentation can be used to mark the beginning of a new web page in an HTTP data stream. The data captured after the Start Segment message will be considered the start of the segment. All data captured after the page will be considered as part of the segment until the next Start Segment message is issued. A Start Segment message can have the properties 791 of Session ID, which uniquely identifies this Session, Start Time, which gives the time at which the segment began, and Segment Data, which can contain data captured from the data stream 105 including, for example, any user input, graphics displayed on the page, and text displayed on the page.

The Include Cached Segments message can instruct the data capture system 205 to include the pre-Start Recording message 712 data stream bytes, which are cached in the data capture system buffer, to be included in the Session VDO content 602.

PLAYBACK CONTROL MESSAGES

Examples of Playback control messages can be used by the control system 120 to inform the data storage system 210, the long term storage system 125, or data capture buffer which recorded sessions or segments are to be retrieved, displayed, or analyzed, as well as to control how those sessions are retrieved, displayed or analyzed.

The Playback message 736 can be used to transmit properties 756 that tell the data storage systems 210 to retrieve and commence viewing or processing of a stored Session indicated by the Record Identifier property. Other properties can be transmitted to the Data storage system indicating how the Session is to be displayed or analyzed, including instructions to display one segment at a time, at the original time intervals, or at a preset time interval, under human interactive control, based upon a filter or search criteria, or other playback methods.

Further, playback control messages can be used by the Control Signal Generator 315 to specify the manner in which the session and its segments are displayed or analyzed. The Session can be displayed or analyzed from the data stream capture buffer, storage system 215, long term storage 125, or a local computer which is hosting the application that is displaying or analyzing the session content and metadata. The storage location of the session to be played back affects how the session is retrieved. Selected stream data in the data capture buffer can be reviewed by the Playback message 736 prior to storage of the session with the Commit message 752.

Use of various Playback control messages allow interactive control of a session playback. The First Segment message 767 displays or loads the first segment of the session according to Sequence Markers 615 into the display or analysis application. The Next Segment message 744 displays or loads the session segment following the

currently loaded segment. The Previous Segment message 760 instructs the system to display or load the session segment preceding the currently loaded segment. The Last Segment message 742 instructs the system to display or load the last segment of the session. The Pause message 784 instructs the displaying or analyzing application to interrupt processing of the session segments on a pre-determined time interval basis until the Playback message 736 is re-transmitted.

STORAGE CONTROL MESSAGES

Examples of Storage control messages can be used by the control system 120 to inform the data storage system 210, the long term storage system 125, or data capture buffer which recorded sessions or segments are to be stored, retrieved, deleted, or edited, as well as to control how these actions are performed.

The Get Record Name message 720 can be used to retrieve the name of a session as stored in the Session object metadata 610 of the VDO 600. This can allow human users to more readily identify a session. The Get Session List message 796 can be used to transmit retrieve all identifiers or a range of identifiers available to a requesting entity for display or analysis. This would allow the requesting entity to better choose the desired session for playback.

The Commit message 752 instructs a storage system 215 or long term storage 125 to write newly captured content segments or newly edited metadata into storage 215 or into long term storage 125. The Delete message 768 instructs a storage system 215 or long term storage 125 to delete a VDO from its storage media. The Delete message can be internally generated by the storage system when the Retention metadata object 635 stipulates that destruction time of the VDO 600 has arrived and the retention period has expired.

Further, Storage control messages beyond those shown in Figure 7 can be used by the Control Signal Generator 315 to specify editing of the values in the metadata objects' 604 properties. The Edit Access message can allow authorized administrators to change VDO access control parameters, Edit Retention messages can allow authorized users to change the destruction date of a VDO, and the Add Externals can allow users and systems to add pertinent externally-sourced metadata to the VDO 600.

The Edit Audit Trail message can be used to add or update audit trail information associated with the VDO 600, including Use History metadata describing access to, editing of, and management of the VDO itself.

GENERAL SESSION MANAGEMENT MESSAGES

General session management messages beyond those shown in Figure 7 can be used to manage other aspects of selective data stream recording that enhance system efficiency, performance, security, reliability, and features.

For example, the User Login message validates that a user or system is an authorized user of the System, and that the user has supplied the correct authentication data. This message can also allow the System to initialize for a new user to selectively record new sessions. A User Login message can contain properties such as User Name, where User Name can contain the textual representation of the name of the user of the system, Validation token, Validation can contain a value that allows the user's authorization to be validated, and Session ID, which can contain a unique identifier for the present data recording session.

Another example is the End Session message, which can inform the data capture system that the current selective recording session will not be capturing any more data from the data stream until the next Start Session command, and that the captured data is in pre-Commit message 752 state and ready for Playback (Review) messages 736. An End Session message can contain the Session ID property, where Session ID can contain a unique identifier for the present data recording session.

The Get Session State message could be used when the control system 120 and the data capture and storage system 220 perform system synchronization. By utilizing this message, the either system component can request the state that the other

component is currently in for this session. A Get Session State message can contain the properties, Session ID, where Session ID can contain a unique identifier for the present data recording session, and Session State, which can contain the current state of the system.

The Reset Session State message can be used to alert the server to reset the state of this session to a predefined condition according to a message property. For example, this message can be equivalent to a combination of the End Session and User Login messages, except the user does not need to validate again to the system in order to start another Session. A Reset Session State message can have the properties Session ID, where Session ID can contain a unique identifier for the present data recording session, and Session State, which can contain the desired state of the system

In another example, The Set Cache Size message can be used to tell the data capture system 205 how many 'cached' segments to save for the session. The cache can be used to capture data stream segments that precede the Start Recording message 712 so that the system user can record data stream segments whose value was not known until the event of subsequent data that made the selective recording of the data stream desirable. This way, otherwise unrecoverable data stream information can be included in the Session VDO content 602. The Set Cache Size message sets the size of the pre-start segment capture buffer in the data capture system 205. This can be important in many situations, including where dynamic content occurs in a data stream (e.g. JavaScript) where the session cannot be replayed. A Set Cache Size message can have the properties Number of Bytes, where the byte number is the amount of data stream bytes to be kept in the data capture system buffer in a circular FIFO queue.

Fig. 8 depicts web page 810 that implements a data recording system according to the present invention. In particular, Fig. 8 shows CommCorder user interface 812. Within user interface 812, a user would have several operations available, including the ability to retrieve a session list using GetSessionList button 815, start playing a session using Playback button 820, start recording using StartRecording button 830, stop recording using StopRecording button 825, and pause the recording using Pause button 835. There can also be several segment controls available to the user, including advancing to the first or last segment using FirstSegment button 840 and LastSegment button 845, advancing to the next segment or previous segment using NextSegment button 850 and PreviousSegment button 855, and deleting a segment using Delete button 860.

While the invention has been described in detail, including references to specific embodiments, it will be apparent to one skilled in the art that changes and modifications can be made to the invention without departing from the spirit and scope thereof. Thus, it is intended that the present invention cover the modifications and variations of this invention provided they come within the scope of the appended claims and their equivalents.

What is claimed is:

1. A method of selectively recording data from a data stream, the method comprising the steps of:

capturing raw data from said data stream;

performing one or more analyses on said raw data;

producing metadata associated with said raw data;

based on said one or more analyses, generating one or more control signals for selecting data to be stored from said raw data; and

storing said selected data and said metadata.

2. A method as in claim 1, wherein said raw data further comprises encrypted data.

3. A method as in claim 2, wherein said step of performing one or more analyses further comprises the step of decrypting said encrypted data.

4. A method as in claim 2, wherein:

said step of performing one or more analyses further comprises the step of identifying one or more cryptographic keys corresponding to said encrypted data; and

said storing step further comprises the step of storing said one or more cryptographic keys.

5. A method of generating control signals for selectively recording data from a data stream over a data network, the method comprising the steps of:

capturing raw data from said data stream;

performing one or more analyses on said raw data;

generating one or more control signals for selecting data to be stored from said raw data; and

transmitting said one or more control signals over said data network.

6. A method as in claim 5, wherein said transmitting step further comprises sending said control signals through a proxy.

7. A method of using control signals to selectively record data from a data stream over a data network, the method comprising the steps of:

receiving said one or more control signals over said data network;

selecting data to be stored from said data stream based on said control signals;

producing metadata associated with said raw data; and

storing said selected data and said metadata.

8. A method of selectively recording data from a data stream within a data processing and transmission system, the method comprising the steps of:

capturing raw data being transmitted between an application server and a presentation server;

creating a copy of said raw data in memory;

collecting metadata associated with said raw data;

delivering said raw data and said metadata to an intermediary server;

queuing said raw data and said metadata for processing;

processing said raw data and said metadata;

creating a verified data object; and

storing said verified data object.

9. A method of using a data recording system to create one or more verified data objects to capture proof of creation and existence of a data stream, comprising the steps of:

receiving a start recording signal;

opening a session identifier;

capturing data, further comprising the steps of:

marking one or more segments;

capturing data from a data stream;

receiving an end segment marker; and

repeating said capturing of data until a pause or stop signal occurs;

generating a close session data packet; and

combining said segments and associated metadata into a verified data object.

10. A method as in claim 9, wherein said combining step further comprises the step of using metadata that includes external context data.

11. A method as in claim 9, wherein said combining step further comprises the step of using metadata that includes system data.

12. A method as in claim 11, wherein said combining step further comprises the step of using system data that includes a machine identification number.

13. A method as in claim 11, wherein said combining step further comprises the step of using system data that includes a media identification number.

14. A method as in claim 9, wherein said combining step further comprises the step of using metadata that includes records management data.

15. A method as in claim 9, wherein said combining step further comprises the step of using metadata that includes access control data.

16. A method as in claim 9, wherein said combining step further comprises the step of using metadata that includes digital auditing data.

17. A method of selectively recording data from a data stream for use in a legacy system environment, the method comprising the steps of:

capturing raw data from said data stream;

performing one or more analyses on said raw data;

producing metadata associated with said raw data;

generating a control signal for selecting data to be stored from said raw data;

converting said metadata and said selected data into an alternative data format; and

storing said converted selected data and said converted metadata.

18. A data recording system, comprising:

a data stream processing system that includes,

an input that receives a data stream from a data network;

an output; and

a control system coupled to said input for selectively passing a subset of data from said data stream to said output; and

a long term data storage device coupled to said output.

19. A data recording system as in claim 18, wherein said data stream processing system further comprises:

a data capture system; and

a data storage system.

20. A data recording system as in claim 19, wherein said data capture system allows said data to be queued for subsequent processing by said control system.

21. A data recording system as in claim 18, wherein said data recording system includes an external system that allows a user to control the data capture process by sending user control signals to said control system.

22. A data recording system as in claim 21, wherein said external system further comprises a user interface.

23. A data recording system as in claim 21, wherein said user control signals further comprise one or more of the signals stop, start, pause, or end.

24. A data recording system as in claim 21, wherein said user control signals further comprise signals permitting processing of data previously stored in said data storage device.

25. A data recording system as in claim 18, wherein said control system further comprises an integrity mechanism.

26. A data recording systems as in claim 25 wherein said integrity mechanism further produces a checksum.

27. A data recording systems as in claim 25 wherein said integrity mechanism further produces a digital signature.

28. A data recording systems as in claim 25 wherein said integrity mechanism limits the ability of a user to alter the recorded data.

29. A data recording system that enables a user to select data for recording by viewing a data stream, comprising:

a user interface that displays said data stream to the user and generates control signals in response to input from said user for selecting data to be recorded;

a control system for receiving said control signals;

a data capture system for temporarily storing selected data from said data stream; and

a data storage system for storing said data.

30. A data recording system as in claim 29 wherein said user interface further comprises a computer display.

31. A data recording system that automatically records selected data from a data stream, comprising:

a data stream analyzer that generates control signals in response to one or more selection criteria for selecting data to be recorded;

a control system for receiving said control signals;

a data capture system for temporarily storing selected data from said data stream; and

a data storage system for storing said data.

32. A data recording system as in claim 31, wherein said data stream analyzer further comprises an automated means for analyzing the content of said data stream.

33. A data recording system for operation over a data network, comprising:

a control system, further comprising:

a local proxy; and

a control signal generator;

one or more intermediary proxies; and

a data capture and storage system, further comprising:

a remote proxy;

a control signal processor;

a metadata generator;

a temporary storage system; and

a long term data storage system;

whereby said control signal generator transmits control messages through said local proxy, said one or more said intermediary proxies, and said remote proxy causing said data capture and storage system to selectively capture data and store said data in said long term data storage system.

34. An object generating system for generating one or more verified data objects that combine selected data from a data stream with associated metadata, comprising:

a control system; and

a data capture and storage system, further comprising:

a control signal processor;

a means for generating metadata;

a temporary storage system; and

a long term data storage system;

whereby said control system transmits control messages causing said data capture and storage system to generate said verified data object and store said verified data object in said long term data storage system.

35. A system as in claim 34, wherein said object generating system further comprises a means for verifying compliance.

36. A system as in claim 35, wherein said means for verifying compliance further comprises a case law compliance verification system.

37. A system as in claim 35, wherein said means for verifying compliance further comprises a regulation compliance verification system.

38. A system as in claim 35, wherein said means for verifying compliance further comprises an audit trail compliance verification system.

39. A system as in claim 34, wherein said means for generating metadata further comprises a system for storing all information necessary to recreate a complete event.

40. A system as in claim 39, wherein said information is further combined into segments.

41. A system as in claim 40, wherein said segments contain HTML information.

42. A system as in claim 40, wherein said segments further comprise dynamic content information.

43. A system as in claim 42, wherein said dynamic content information further comprises executable computer code embedded in the recorded data stream.

44. A system as in claim 43, wherein said executable computer code further comprises one or more JavaScript objects.

45. A system as in claim 40, wherein said segments further comprise encryption keys.

46. A system as in claim 40, wherein said segments further comprise indices for searching previously recorded data.

47. A system as in claim 40, wherein said segments further comprise XML data tags.

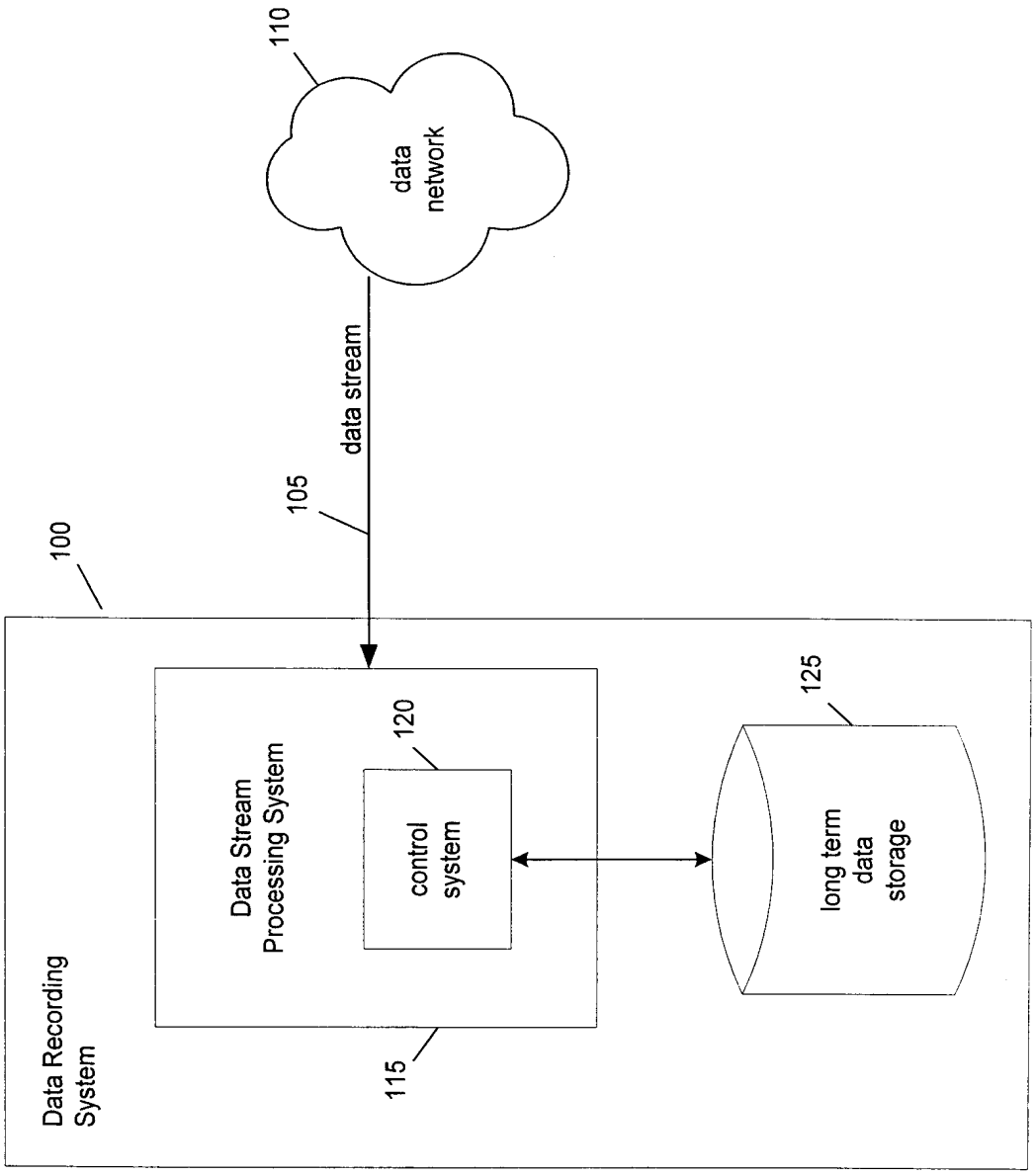

110
data network
data stream
105
100
Data Recording System
Data Stream Processing System
120
control system
125
long term data storage
115

Figure 1

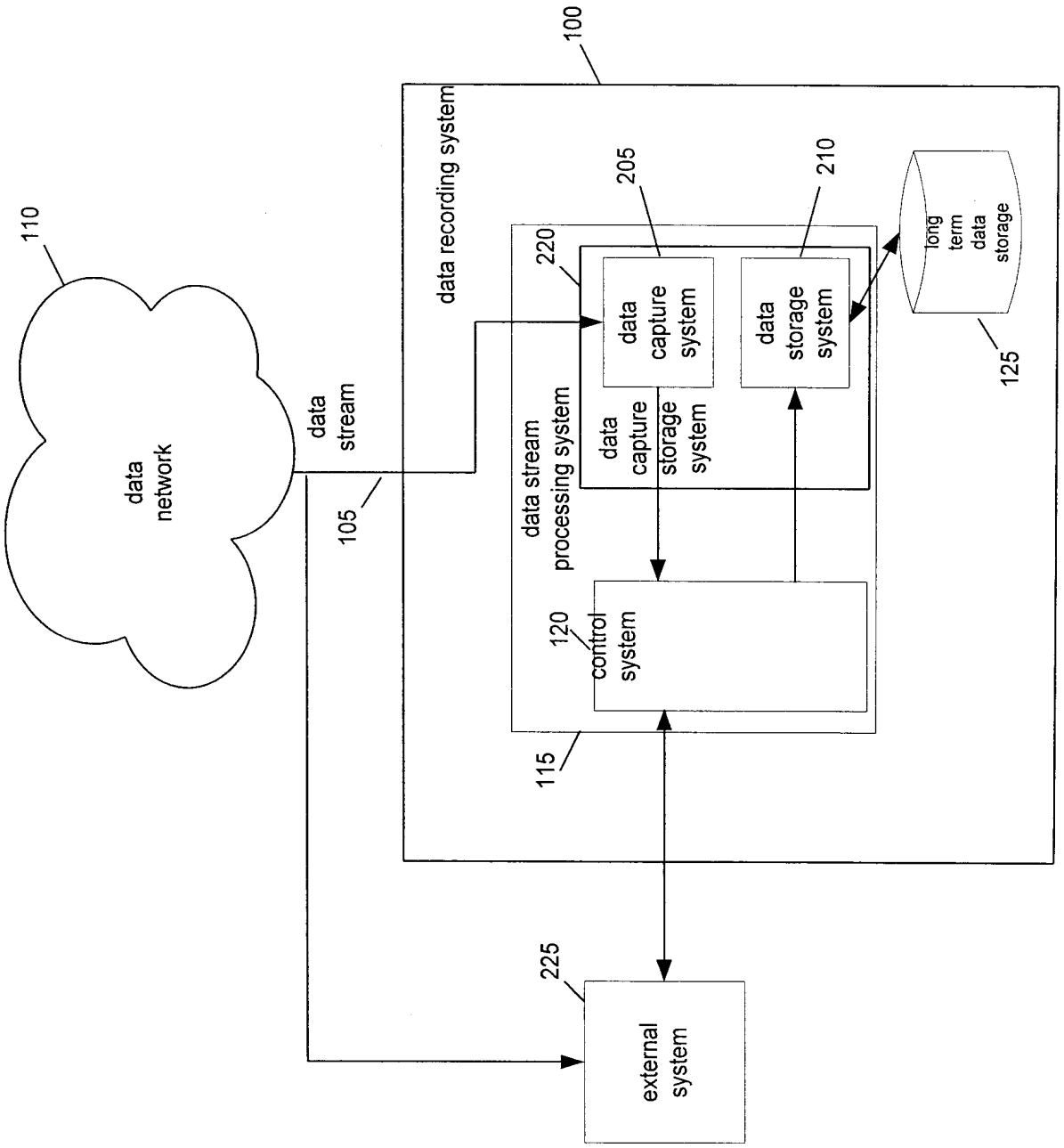

100
data recording system
110
data network
data stream
105
205
210
220
data capture system
data storage system
long term data storage
125
data stream processing system
data capture storage system
120
control system
115
225
external system

Figure 2a

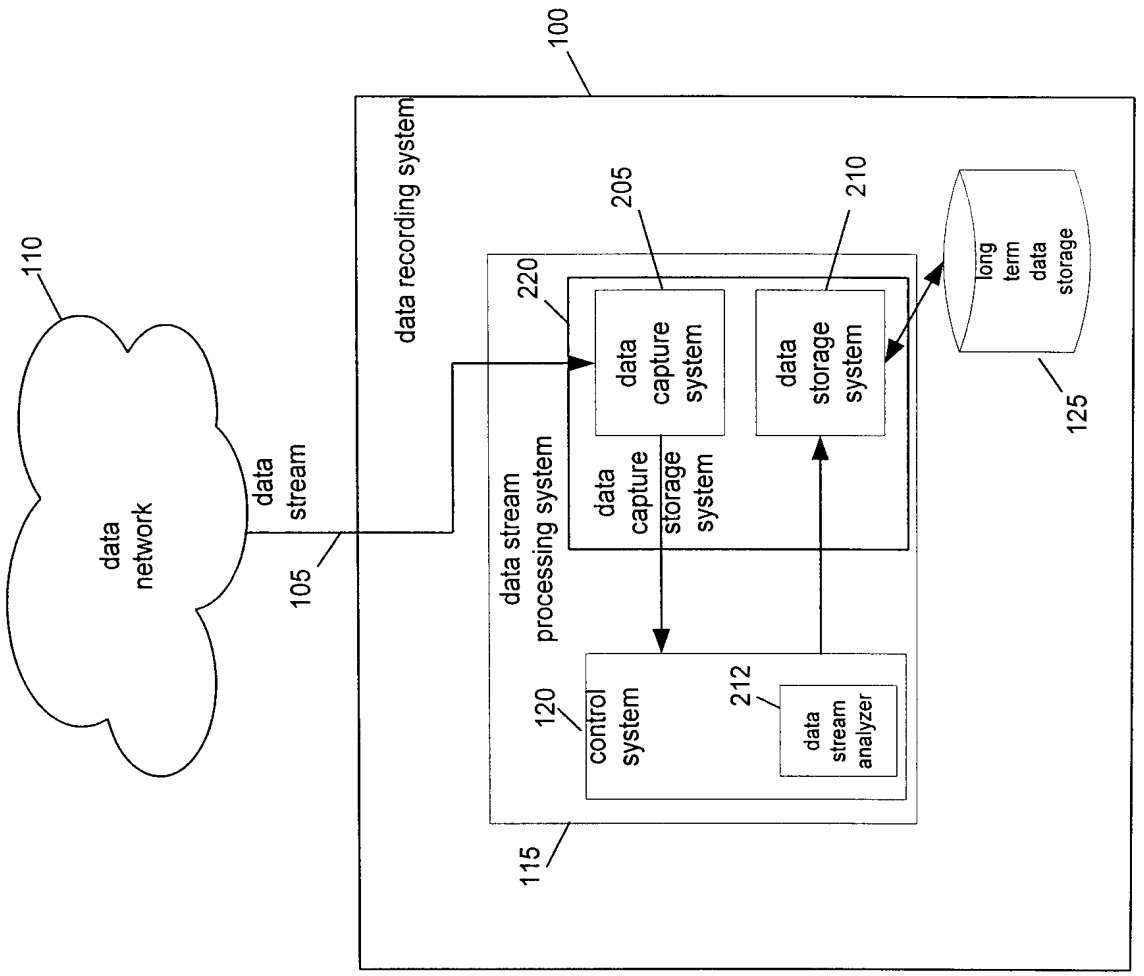

100
data recording system
110
data network
data stream
105
205
210
220
data capture system
data storage system
long term data storage
125
data stream processing system
data capture storage system
120
control system
212
data stream analyzer
115

Figure 2b

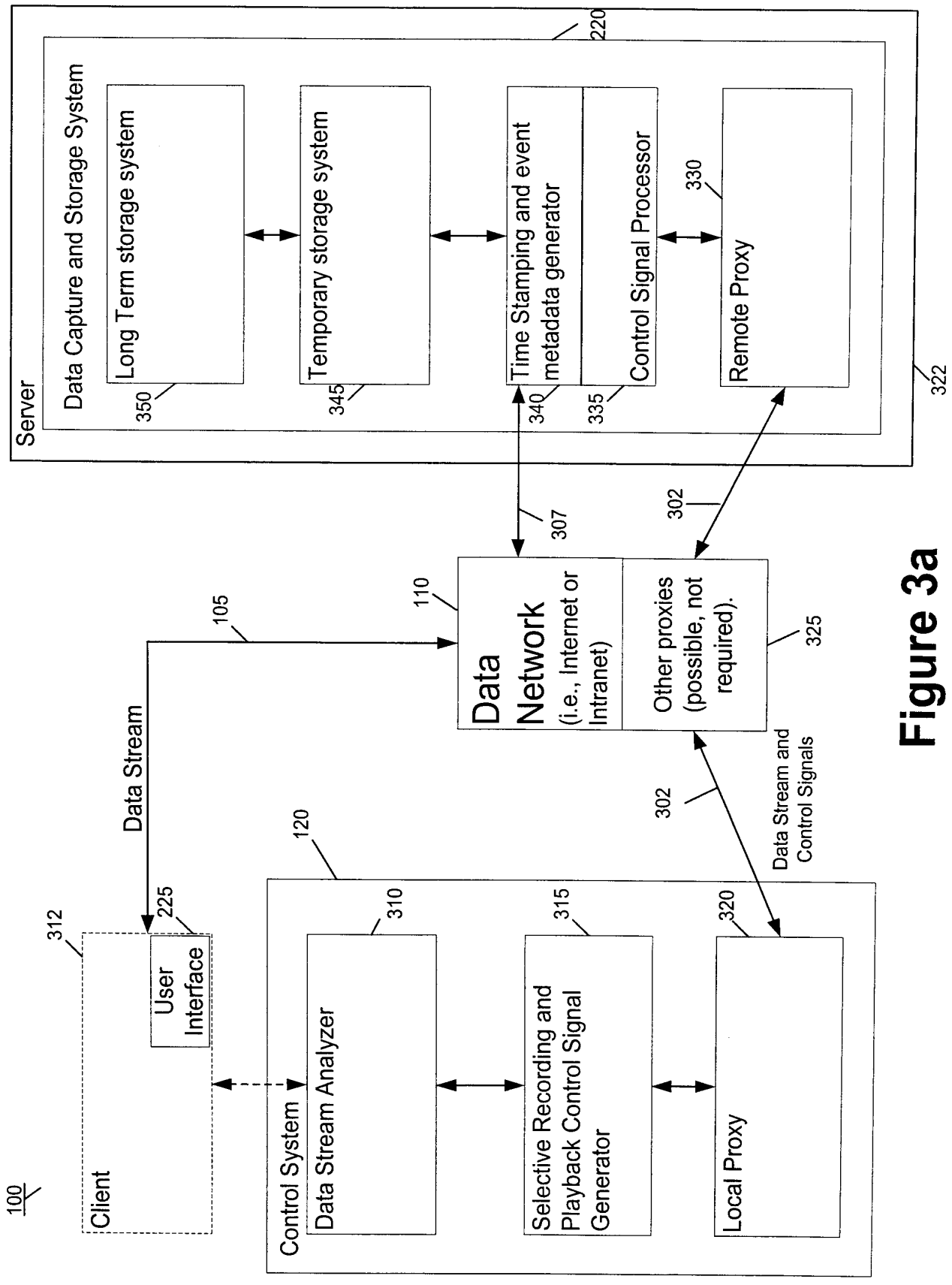

Server
Data Capture and Storage System
Long Term storage system
Temporary storage system
Time Stamping and event metadata generator
Control Signal Processor
Remote Proxy
220
350
345
340
335
330
322
307
302
105
110
Data Stream
Data Network (i.e., Internet or Intranet)
Other proxies (possible, not required).
325
302
Data Stream and Control Signals
120
312
225
User Interface
Client
Control System
Data Stream Analyzer
310
Selective Recording and Playback Control Signal Generator
315
Local Proxy
320
100

Figure 3a

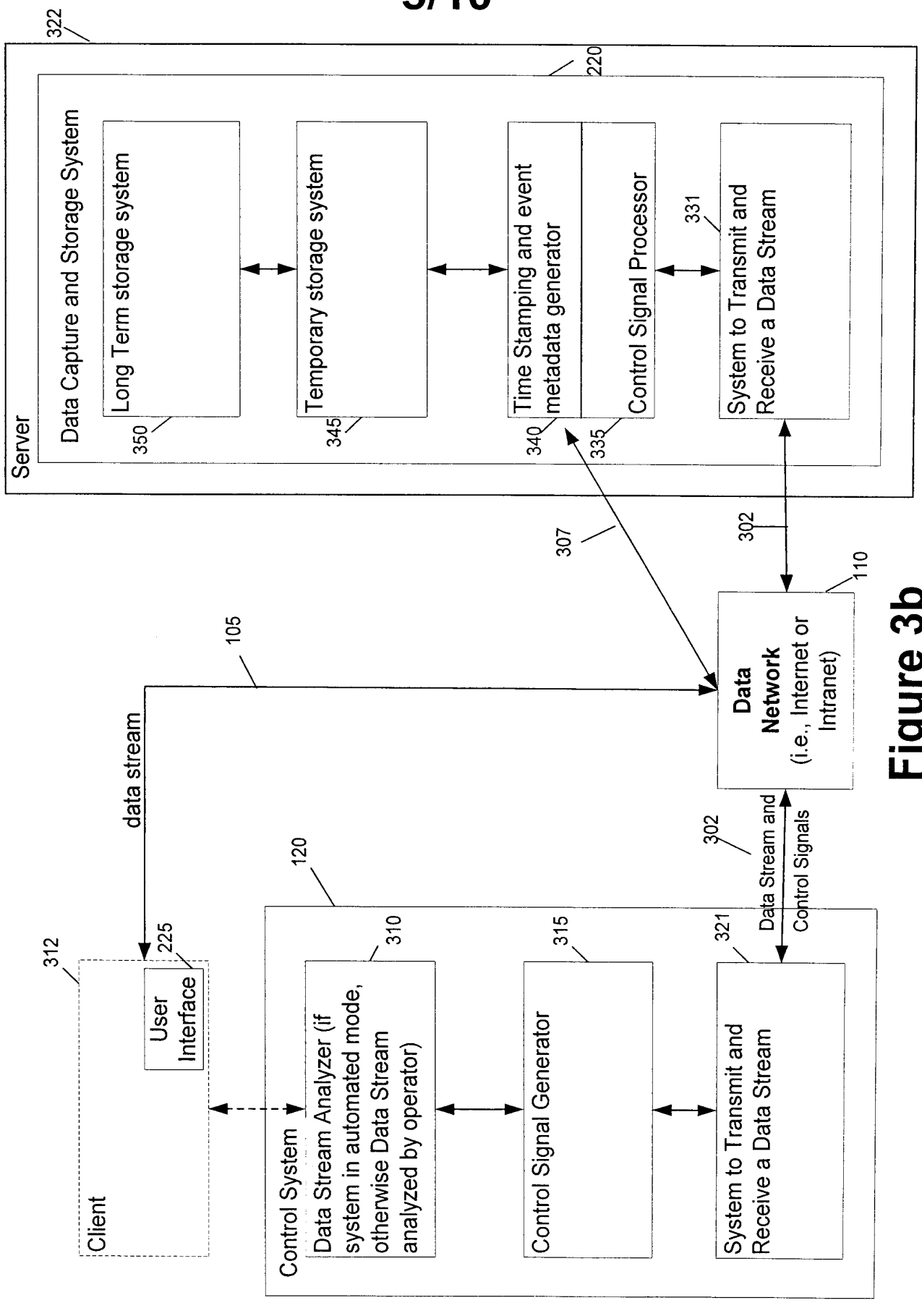

322
Server
220
Data Capture and Storage System
Long Term storage system
350
Temporary storage system
345
Time Stamping and event metadata generator
340
Control Signal Processor
335
331
System to Transmit and Receive a Data Stream
307
302
110
Data Network (i.e., Internet or Intranet)
105
data stream
120
302
Data Stream and Control Signals
312
225
User Interface
Client
Control System
Data Stream Analyzer (if system in automated mode, otherwise Data Stream analyzed by operator)
310
Control Signal Generator
315
321
System to Transmit and Receive a Data Stream

Figure 3b

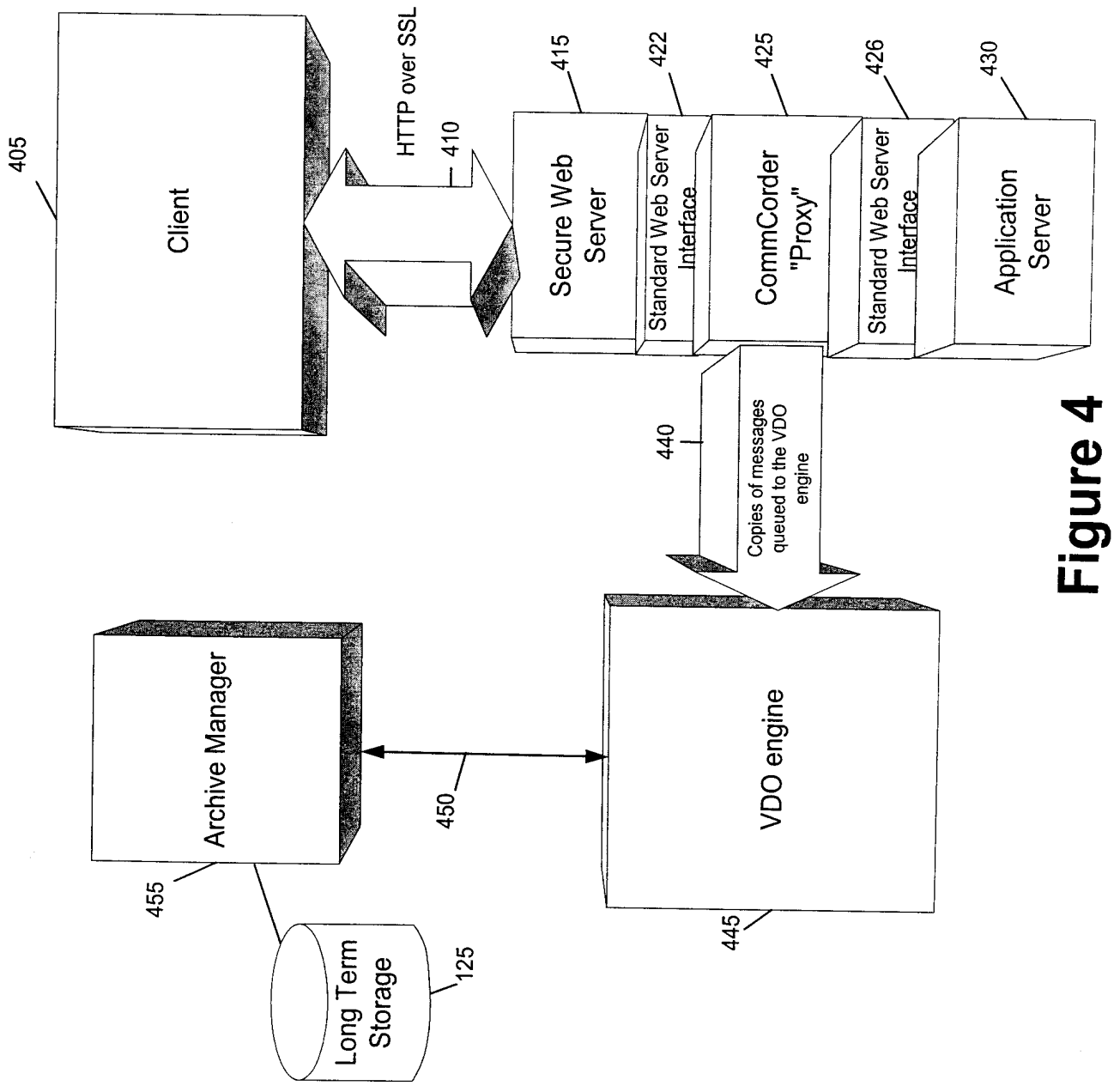

Client
405
HTTP over SSL
410
Secure Web Server
415
Standard Web Server Interface
422
CommCorder "Proxy"
425
Standard Web Server Interface
426
Application Server
430
Copies of messages queued to the VDO engine
440
Archive Manager
455
Long Term Storage
125
450
VDO engine
445

Figure 4

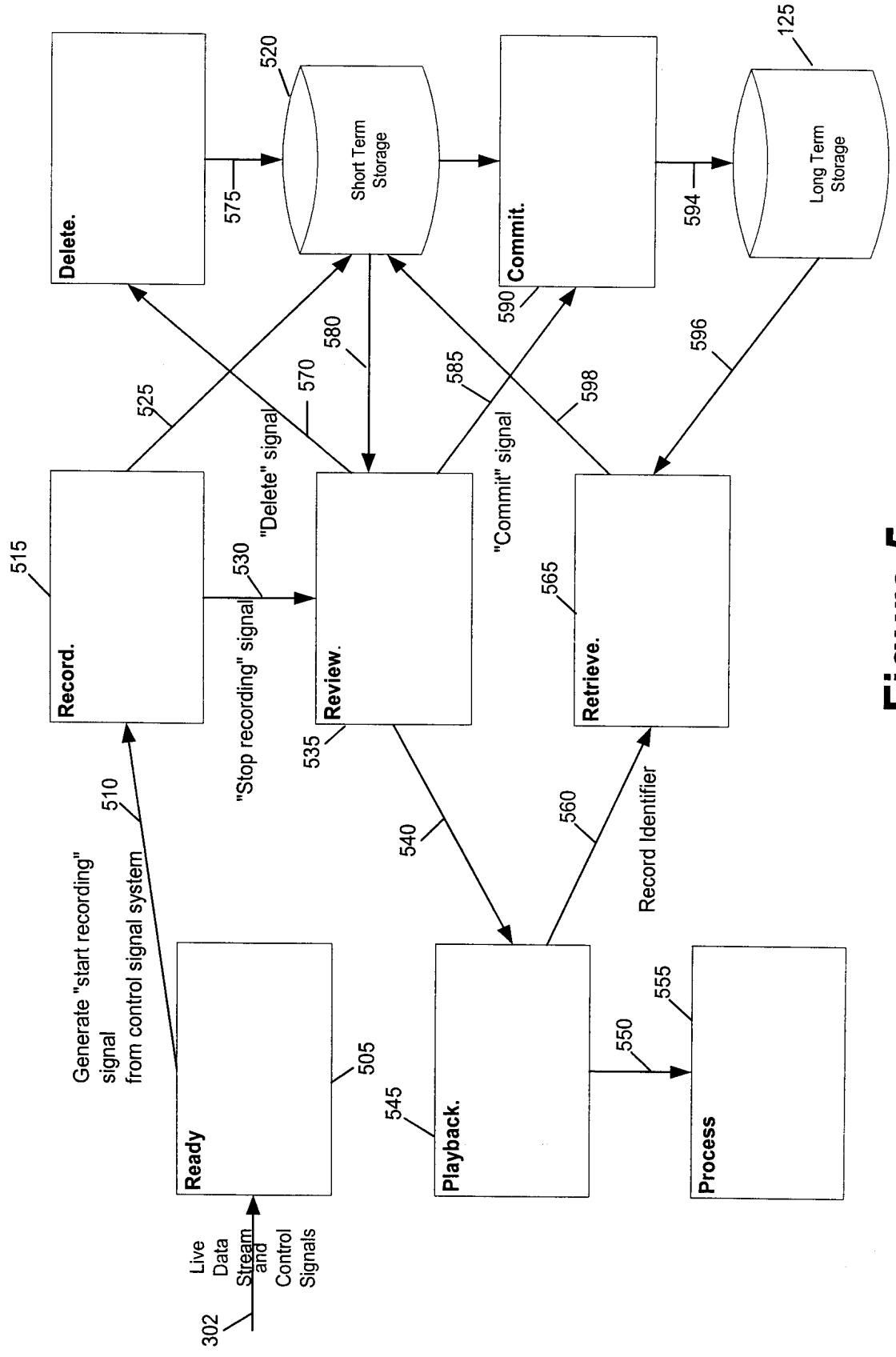

Delete.
520
Short Term Storage
Commit.
125
Long Term Storage
575
594
590
580
570
585
598
596
525
"Delete" signal
"Commit" signal
515
Record.
530
Review.
565
Retrieve.
"Stop recording" signal
535
510
Generate "start recording" signal from control signal system
540
560
Record Identifier
Ready
505
Playback.
545
550
555
Process
Live Data Stream and Control Signals
302

Figure 5

8/10

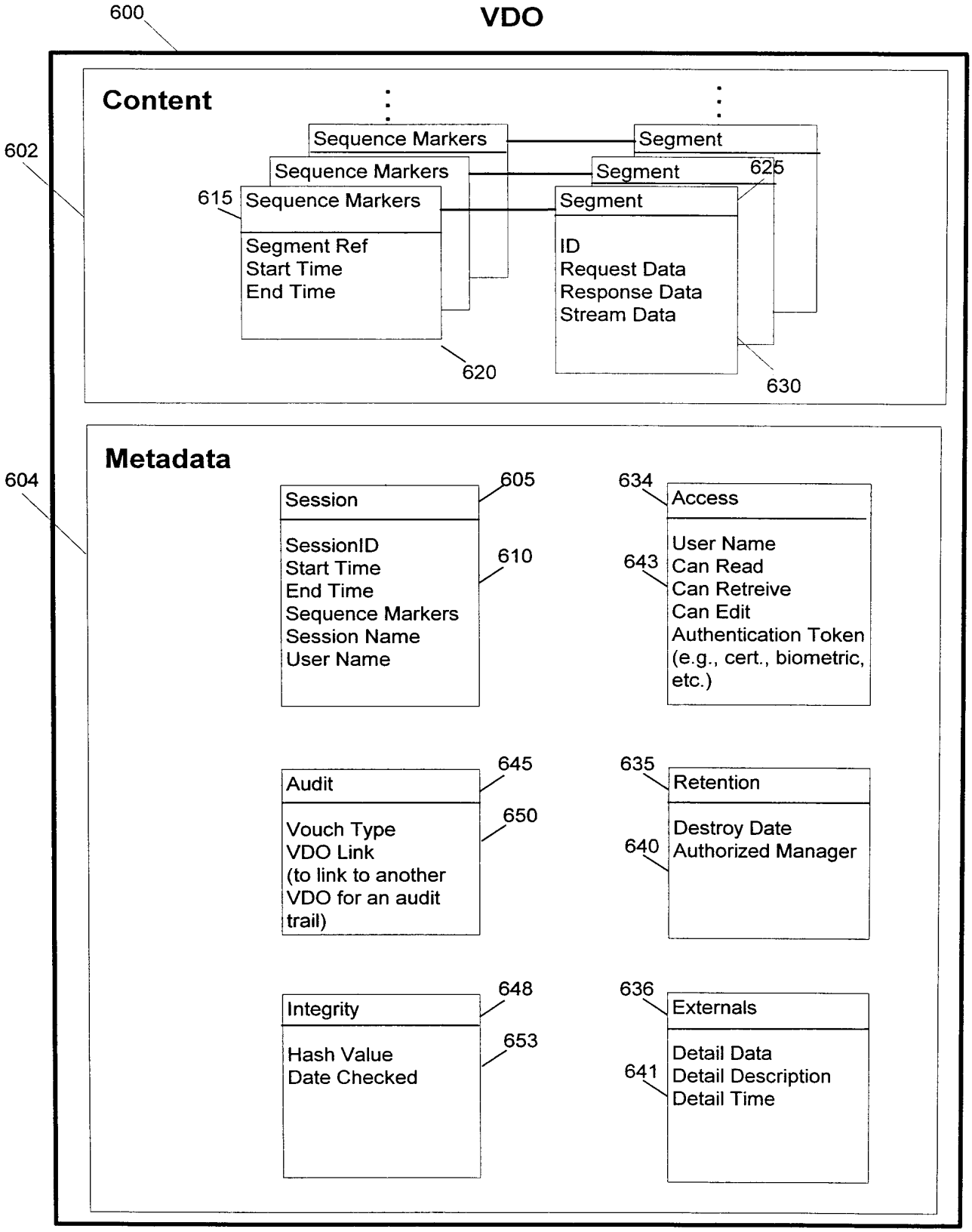

600
VDO
Content
602
Sequence Markers
Sequence Markers
615
Sequence Markers
Segment Ref
Start Time
End Time
620
Segment
Segment
625
Segment
ID
Request Data
Response Data
Stream Data
630
Metadata
604
Session
605
SessionID
Start Time
End Time
Sequence Markers
Session Name
User Name
610
634
Access
User Name
643
Can Read
Can Retreive
Can Edit
Authentication Token
(e.g., cert., biometric, etc.)
Audit
645
Vouch Type
VDO Link
(to link to another VDO for an audit trail)
650
635
Retention
Destroy Date
640
Authorized Manager
Integrity
648
Hash Value
Date Checked
653
636
Externals
Detail Data
641
Detail Description
Detail Time

Figure 6

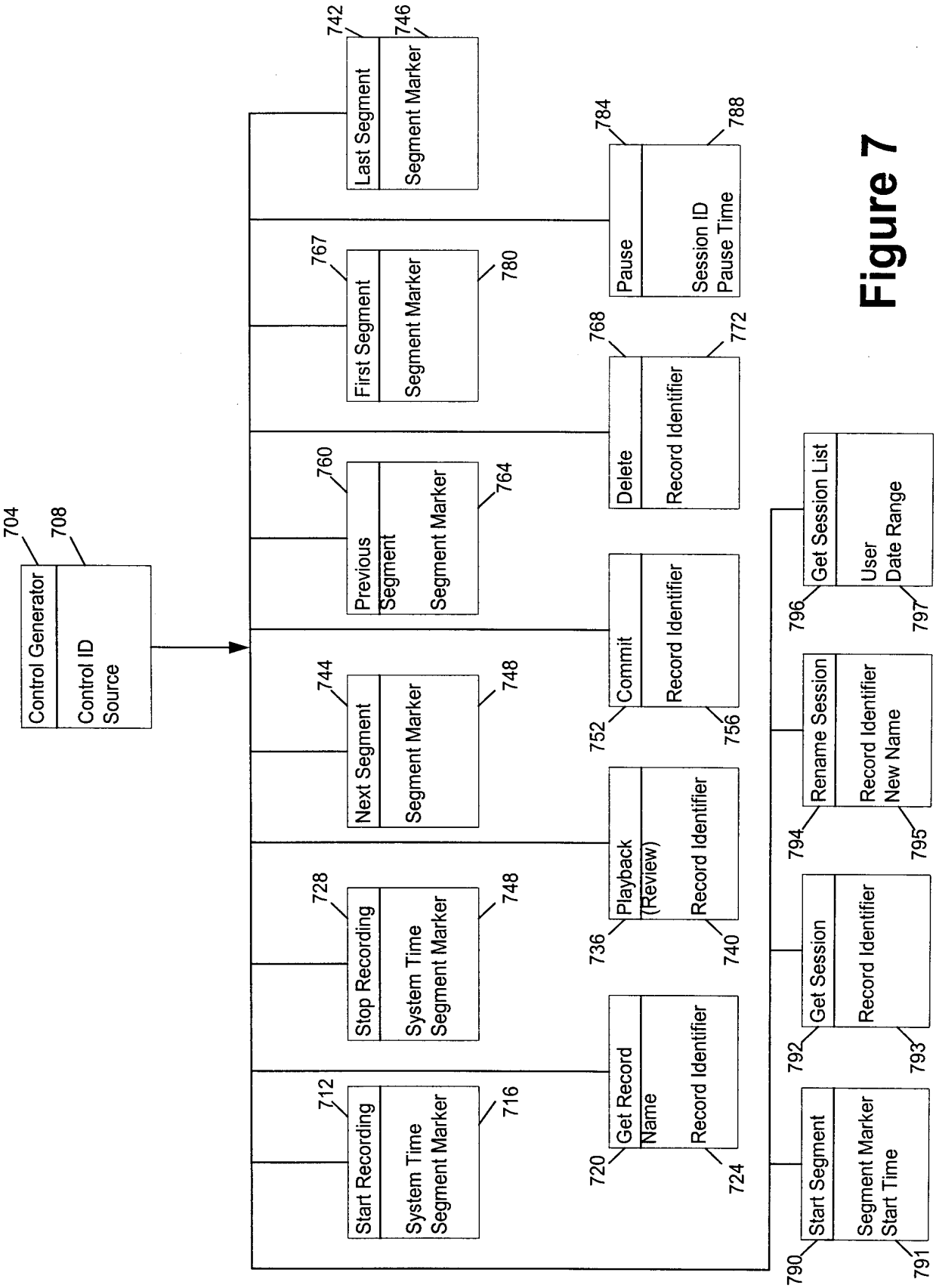

704
708
Control Generator
Control ID Source
712
Start Recording
System Time Segment Marker
716
728
Stop Recording
System Time Segment Marker
748
744
Next Segment
Segment Marker
748
760
Previous Segment
Segment Marker
764
767
First Segment
Segment Marker
780
742
746
Last Segment
Segment Marker
720
Get Record
Name
Record Identifier
724
736
Playback (Review)
Record Identifier
740
752
Commit
Record Identifier
756
768
Delete
Record Identifier
772
784
Pause
Session ID
Pause Time
788
790
Start Segment
Segment Marker
Start Time
791
792
Get Session
Record Identifier
793
794
Rename Session
Record Identifier
New Name
795
796
Get Session List
User
Date Range
797

Figure 7

10/10

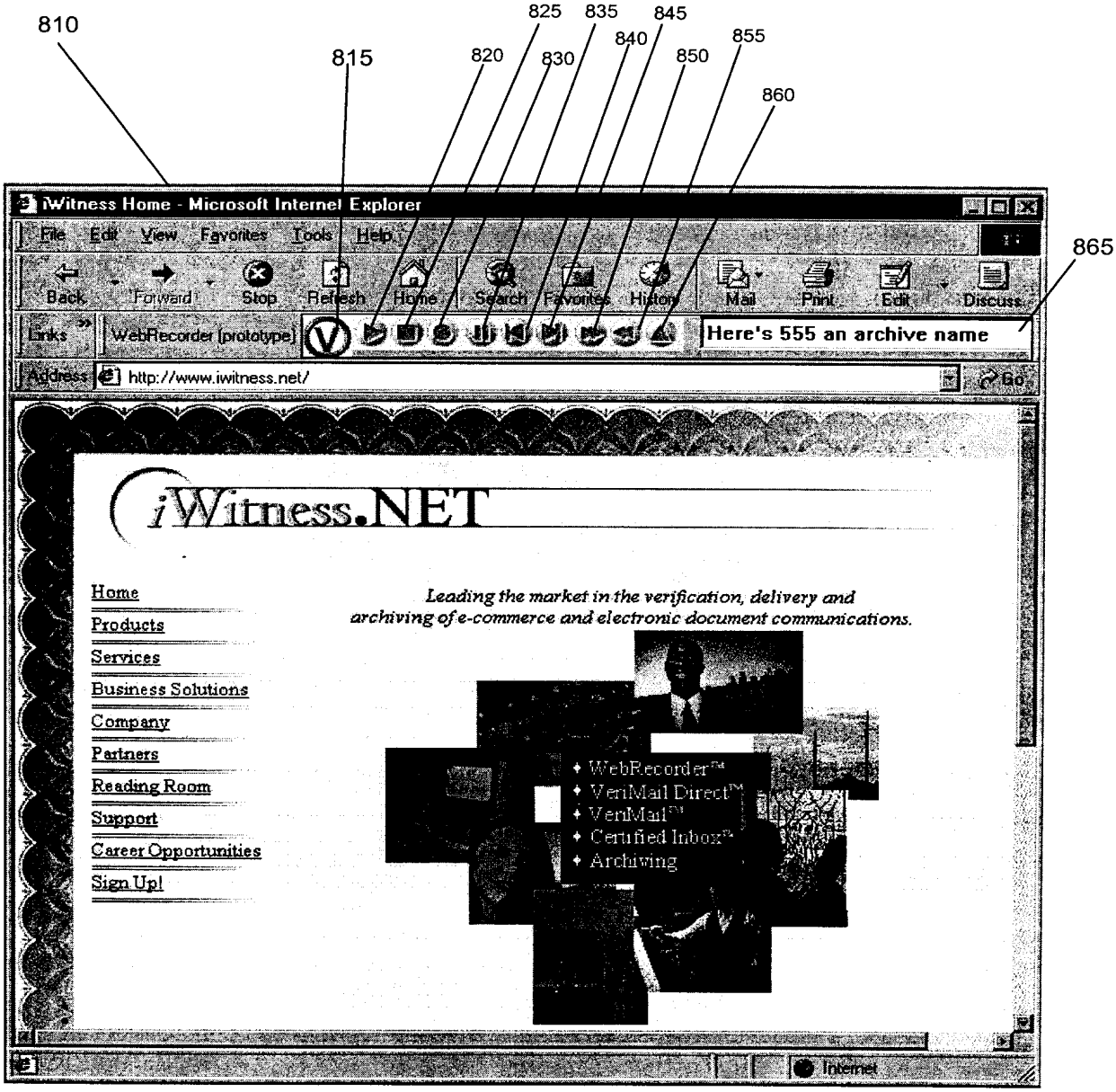


Figure 8